



Håndbok for administrasjon av bordmodeller

Stasjonære forretnings-PCer

Dokumentets delnummer: 312947-092

September 2003

Denne håndboken gir definisjoner og instruksjoner om hvordan du bruker funksjoner for sikkerhet og Intelligent administrasjon som er forhåndsinstallert på enkelte modeller.

© 2003 Hewlett-Packard Development Company, L.P.

HP, Hewlett Packard og Hewlett Packard-logoen er varemerker som tilhører Hewlett-Packard Company i USA og andre land.

Compaq og Compaq-logoen er varemerker som tilhører Hewlett-Packard Development Company, L.P. i USA og andre land.

Microsoft, MS-DOS, Windows og Windows NT er varemerker som tilhører Microsoft Corporation i USA og andre land.

Alle andre produktnavn som er nevnt i dette dokumentet, kan være varemerker som tilhører de respektive selskaper.

Hewlett-Packard Company skal ikke være ansvarlig for tekniske feil eller redigeringsfeil eller utelatelser i dette dokumentet, eller indirekte skade eller følgeskader i forbindelse med utgivelsen, ytelsen eller bruken av dette materialet. Informasjonen i dette dokumentet formidles som den er ("as is") og uten garanti av noe slag, herunder, men ikke begrenset til, implisitte garantier for salgbarhet eller egnethet for et bestemt formål, og kan endres uten varsel. Garantien for HP-produkter er fremsatt i de uttrykkelige garantierklæringene som følger med slike produkter. Intet i dette dokumentet må oppfattes som om det innebærer en tilleggsgaranti.

Dette dokumentet inneholder privat informasjon som er opphavsrettslig beskyttet. Ingen del av dette dokumentet kan fotokopieres, mangfoldiggjøres eller oversettes til et annet språk uten at det foreligger skriftlig tillatelse fra Hewlett-Packard Company.



ADVARSEL: Tekst som er markert på denne måten, angir at hvis anvisningene ikke blir fulgt, kan det føre til personskade eller livsfare.



FORSIKTIG! Tekst som er markert på denne måten, angir at hvis anvisningene ikke blir fulgt, kan det føre til skade på utstyr eller tap av data.

Håndbok for administrasjon av bordmodeller

Stasjonære forretnings-PCer

Annen utgave (September 2003)
Dokumentets delnummer: 312947-092

Innhold

Håndbok for administrasjon av bordmodeller

Første konfigurasjon og distribusjon	2
Fjernsysteminstallasjon	3
Oppdatering og administrasjon av programvare	4
HP Client Manager Software	4
Altiris Solutions	4
Altiris PC Transplant Pro	5
System Software Manager	6
Proactive Change Notification	6
ActiveUpdate	6
ROM-Flash	7
Fjern-ROM-Flash	7
HPQFlash	8
FailSafe Boot Block ROM	8
Kopiere Setup	9
Strømbryter med dobbelt funksjon	18
Nettsted	19
Byggekløsser og partnere	19
Aktivasporing og sikkerhet	20
Passordsikkerhet	24
Etablere et konfigureringspassord ved hjelp av Computer Setup.	24
Opprette et oppstartspassord ved hjelp av Computer Setup	25
Innebygd sikkerhet	29
DriveLock	37
Smart dekselsensor	40
Smart deksellås	41
Master Boot Record-sikkerhet	43

Før du partisjonerer eller formaterer gjeldende oppstartbare disk	45
Kabellåsutstyr	45
Teknologi for identifikasjon av fingeravtrykk	46
Varsling og reparering av feil	46
System for harddiskbeskyttelse	46
Overspenningstolerant strømforsyning	47
Varmesensor	47

Register

Håndbok for administrasjon av bordmodeller

HP Intelligent administrasjon gir deg standardbaserte løsninger for administrasjon og kontroll av bord-PCer, arbeidsstasjoner og bærbar PCer i et nettverksmiljø. HP var banebrytende innen administrasjon av bordmodeller i 1995, da de introduserte bransjens første fullstendig administrerbare stasjonære personlige datamaskiner. HP har en patent på administrasjonsteknologien. Siden da har HP ledet et bransjeomfattende arbeid med å utvikle de nødvendige standardene og infrastruktur for å distribuere, konfigurere og administrere arbeidsstasjoner og bærbar PCer på en effektiv måte. HP arbeider tett med leverandører av ledende administrasjonsprogramvareløsninger i bransjen for å sikre kompatibilitet mellom Intelligent administrasjon og disse produktene. Intelligent administrasjon er et viktig aspekt i vår omfattende satsning på å kunne tilby deg PC-administrasjonsløsninger for livssyklusen som hjelper deg med de fire fasene i livssyklusen til en stasjonær PC – planlegging, distribusjon, behandling og overganger.

De viktigste egenskapene ved og funksjonene til administrasjon av bordmodeller er:

- Første konfigurasjon og distribusjon
- Fjernsysteminstallasjon
- Oppdatering og administrasjon av programvare
- ROM-flash
- Aktivasjon og sikkerhet
- Varsling og reparasjon av feil



Støtten for bestemte funksjoner beskrevet i denne håndboken, kan variere etter modell og programvareversjon.

Første konfigurasjon og distribusjon

Datamaskinen din leveres med et forhåndsinstallert systemprogramvarebilde. Etter en kort utpakkingsprosess for programvaren er datamaskinen klar til bruk.

Du foretrekker kanskje å erstatte det forhåndsinstallerte programvarebildet med et tilpasset sett med system- og bruksprogramvare. Det finnes flere måter å spre et tilpasset programvarebilde på. Disse kan være:

- Installere tilleggsprogrammer etter at det forhåndsinstallerte programvarebildet er pakket ut.
- Bruke verktøy for programvaredistribusjon, for eksempel Altiris Deployment Solution™, til å erstatte den forhåndsinstallerte programvaren med et tilpasset programvarebilde.
- Bruke en diskkloningsprosess til å kopiere innhold fra en harddisk til en annen.

Hvilken spredningsmetode som er best, avhenger av informasjonsteknologimiljøet og -prosessene som gjelder for deg. Informasjon som hjelper deg med å velge den beste distribusjonsmetoden, finner du på nettstedet for HP Lifecycle Solutions (<http://h18000.www1.hp.com/solutions/pcsolutions>).

Restore Plus! -CDen, ROM-basert konfigurasjon og ACPI-maskinvare gir ytterligere assistanse med gjenoppbygging av systemprogramvare, konfigurasjonsadministrasjon og feilsøking, og strømstyring.

Fjernsysteminstallasjon

Fjernsysteminstallasjon gjør det mulig å starte og konfigurere maskinen ved hjelp av informasjonen om programvare og konfigurasjon som ligger på en nettverksserver, ved å starte PXE (Preboot Execution Environment). Fjernsysteminstallasjonen brukes vanligvis som et verktøy for systeminnstilling og konfigurering, og kan brukes til å utføre følgende oppgaver:

- Formaterer en harddisk
- Distribuerer et programvarebilde på én eller flere nye PCer
- Fjernoppdatering av systemets BIOS i flash-ROM
(["Fjern-ROM-Flash" på side 7](#))
- Konfigurere systemets BIOS-innstillinger

For å sette i gang fjernsysteminstallasjon trykker du på **F12** når meldingen F12 = Network Service Boot vises nederst i høyre hjørne av HP-logoskjermbildet. Fortsett prosessen ved å følge anvisningene på skjermen. Standard oppstartsrekkefølge er en BIOS-konfigurasjonsinnstilling som kan endres til alltid å forsøke en PXE-oppstart.

HP og Altiris, Inc. er sammen om å tilby verktøy som er utformet for å gjøre distribusjon og behandling av firma-PCer enklere og mindre tidkrevende, slik at de totale kostnadene ved eierskap til slutt reduseres og gjør HP PCene til de mest administrasjonsvennlige klient-PCene for firmamiljøet.

Oppdatering og administrasjon av programvare

HP leverer flere verktøy for administrasjon og oppdatering av programvare på bordmodeller og arbeidsstasjoner – Altiris; Altiris PC Transplant Pro; HP Client Manager Software, en Altiris-løsning; System Software Manager; Proactive Change Notification og ActiveUpdate.

HP Client Manager Software

Intelligent HP Client Manager Software (HP CMS) integrerer HP Intelligent Manageability technology tett med Altiris for å yte overlegne funksjoner for maskinvareadministrasjon for HP-tilgangsenheter, som blant annet disse:

- Detaljerte visninger av maskinvarebeholdningen for aktivastyring
- PC-helsesjekk med overvåkning og diagnose
- Proaktiv varsling om forandringer i maskinvaremiljøet
- Internett- tilgjengelig rapportering av forretningskritiske detaljer som for eksempel maskiner med overopphetingsadvarsler, minnevarsler og annet
- Fjernoppdatering av systemprogrammer som enhetsdrivere og ROM BIOS
- Ekstern endring av oppstartrekkefølgen

Hvis du vil ha mer informasjon om HP Client Manager, kan du besøke http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Solutions

HP Client Management-løsninger gir sentralisert maskinvareadministrasjon av HPs klientenheter for alle IT-levetidsområder.

- Administrasjon av lagerhold og aktiva
 - ❑ Kompatibilitet for programvarelisens
 - ❑ PC-sporing og -rapportering
 - ❑ Leasing-kontrakt, fastsetter aktivasporing
- Distribusjon og migrering
 - ❑ Microsoft Windows 2000-, Windows XP Professional- eller Home Edition-migrering
 - ❑ Systemdistribusjon
 - ❑ Personalitetsmigreringer

- Help Desk og problemløsning
 - ❑ Administrere Help Desk-billetter
 - ❑ Ekstern problemløsning
 - ❑ Ekstern problemløsning
 - ❑ Katastrofe-gjenoppretting for klient
- Administrasjon av programvare og drift
 - ❑ Kontinuerlig administrasjon av bordmodeller
 - ❑ Programvaredistribusjon for HP-system
 - ❑ Egenheling for applikasjon

På utvalgte skrivebords- og notebook-modeller er en Altiris-administrasjonsagent inkludert som en del av det fabrikklastede bildet. Denne agenten muliggjør kommunikasjon med Altiris Development-løsningen som kan brukes til å komplettere ny maskinvaredistribusjon eller personlighetsmigrering til et nytt operativsystem ved hjelp av veivisere som er enkle å følge. Altiris-løsningene inneholder lettvinde funksjoner for programvaredistribusjon. Når det brukes sammen med SSM (System Software Manager) eller HP Client Manager, kan administratorer også oppdatere ROM BIOS og programvare for enhetsdrivere fra en sentral konsoll.

Se <http://www.hp.com/go/easydeploy> for mer informasjon.

Altiris PC Transplant Pro

Altiris PC Transplant Pro gir deg problemfri PC-migrering ved at det bevarer gamle innstillinger, preferanser og data, og migrerer dem hurtig og lettvtint til det nye miljøet. Oppgraderingen er gjort på minutter i stedet for timer eller dager som tidligere, og PCen og programmene virker og ser ut akkurat slik brukerne venter.

Hvis du vil ha mer informasjon og opplysninger om hvordan du laster ned en fullt ut funksjonell 30-dagers evalueringsversjon, kan du besøke <http://h18000.www1.hp.com/im/prodinfo.html#deploy>.

System Software Manager

System Software Manager (SSM) er et verktøy som du kan bruke til å oppdatere programvare på maskinnivå på flere maskiner samtidig. Når SSM blir utført på en klientmaskin, registreres både maskinvare- og programvareversjoner, og deretter oppdateres den riktige programvaren fra et sentralt oppbevaringssted, som også kalles et fillager. Driverversjoner som støttes av SSM, er markert med et spesielt ikon på nettstedet for nedlasting av drivere og på Støtteprogramvare-CDen. Hvis du vil laste ned verktøyet eller få mer informasjon om SSM, kan du besøke <http://h18000.www1.hp.com/im/ssmwp.html>.

Proactive Change Notification

Programmet Proactive Notification bruker nettstedet Subscriber's Choice for å utføre følgende proaktivt og automatisk:

- Sende e-postmeldinger om proaktive endringer (PCN) som varsler deg om maskin- og programvareendringer for de fleste kommersielt tilgjengelige datamaskiner og servere, opptil 60 dager på forhånd.
- Sende deg e-post med kundebulletiner, kunderåd, kundemerknader, sikkerhetsbulletiner og drivervarsler for de fleste kommersielt tilgjengelige datamaskiner og servere.

Du oppretter din egen profil for å sikre at bare du mottar den informasjonen som er relevant for et spesifikt IT-miljø. Hvis du vil vite mer om programmet Proactive Change Notification og opprette en egendefinert profil, kan du besøke <http://www.hp.com/go/pcn>.

ActiveUpdate

ActiveUpdate er et klientbasert program fra HP. ActiveUpdate-klienten kjører på det lokale systemet og bruker den brukerdefinerte profilen til proaktivt og automatisk å laste ned programvareoppdateringer for de fleste kommersielle datamaskiner og servere fra HP. Disse nedlastede programvareoppdateringene kan distribueres intelligently til maskinene de er beregnet på, ved hjelp av HP Client Manager Software og System Software Manager.

Hvis du vil lese mer om ActiveUpdate, laste ned programmet og opprette en tilpasset profil, kan du besøke <http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html>.

ROM-Flash

Datamaskinen leveres med en programmerbar Flash-ROM (read only memory). Ved å opprette et konfigureringspassord i Computer Setup (F10) beskytter du ROMen mot utilsiktet oppdatering eller overskriving. Dette er viktig for å sikre datamaskinens driftsintegritet. Hvis du ønsker eller trenger å oppgradere ROM-minnet, kan du:

- Bestille en oppgradert ROMPaq-diskett fra HP.
- Laste ned de siste ROMPaq-bildene fra <http://h18000.www1.hp.com/im/ssmwp.html>.



FORSIKTIG! For å få maksimal ROM-beskyttelse må du etablere et konfigureringspassord. Konfigureringspassordet hindrer uautoriserte oppgraderinger av ROMen. System Software Manager gjør systemadministratoren i stand til å definere konfigureringspassordet på en eller flere PCer samtidig. For mer informasjon, besøk <http://h18000.www1.hp.com/im/ssmwp.html>.

Fjern-ROM-Flash

Ved hjelp av Fjern-ROM-Flash kan systemadministratoren trygt oppgradere ROMen på fjerntilkoblede HP-PCer direkte fra det sentraliserte nettverksstyringskonsollet. Det at systemansvarlig kan utføre denne oppgaven fra en ekstern maskin på flere datamaskiner og PCer, gir en konsekvent distribusjon av og bedre kontroll over HP PC ROM-bilder over nettverket. Det gir også større produktivitet og lavere eierkostnader.



Datamaskinen må være slått på, eller startet ved Fjernoppstart, for at du skal kunne benytte deg av Fjern-ROM-Flash.

Hvis du vil ha mer informasjon om fjern-ROM-Flash, kan du se i HP Client Manager Software eller System Software Manager på <http://h18000.www1.hp.com/im/prodinfo.html>.

HPQFlash

HPQFlash-verktøyet brukes til lokal oppdatering eller gjenoppretting av systemet-ROM på individuelle PCer gjennom et Windows-operativsystem.

Hvis du vil ha mer informasjon om HPQFlash, kan du besøke <http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html>.

FailSafe Boot Block ROM

FailSafe Boot Block ROM gir mulighet for gjenoppretting av systemet hvis det mot formodning skulle oppstå svikt i ROM-Flash-funksjonen, hvis det for eksempel skulle skje et strømbrudd under en ROM-oppgradering. Boot Block er en Flash-beskyttet del av ROMen som kontrollerer at det finnes et gyldig system-ROM-flash når strømforsyningen til systemet slås på.

- Hvis system-ROM-en er gyldig, starter systemet på normal måte.
- Hvis system-ROM-en ikke passerer gyldighetskontrollen, vil FailSafe Boot Block ROM gi nok støtte til å starte systemet fra en ROMPaq-diskett, som vil programmere system-ROM-en med et gyldig bilde.

Når Bootblock oppdager et ugyldig system-ROM, blinker systemstrømlampen RØDT 8 ganger med ett sekunds mellomrom, etterfulgt av en pause på 2 sekunder. Det lyder også 8 samtidige lydsignaler. En melding om Boot Block gjenopprettingsmodus vises på skjermen (enkelte modeller).

Når du skal gjenopprette systemet etter at det går inn i Boot Block gjenopprettingsmodus, gjør du følgende:

1. Hvis det står en diskett i diskettstasjonen, tar du ut disketten og slår av strømmen.
2. Sett en ROMPaq-diskett inn i diskettstasjonen.
3. Slå på strømmen til systemet.
4. Hvis det ikke blir funnet noen ROMPaq-diskett, blir du bedt om å sette inn en og starte datamaskinen på nytt.
5. Hvis det er opprettet et konfigureringspassord, vil Caps Lock-lyset bli slått på og du blir bedt om å taste inn passordet.

6. Tast inn konfigureringspassordet.
7. Hvis systemet klarer å starte fra disketten og omprogrammere ROM-en, vil de tre tasturlampene lyse. En serie lydsignaler i stigende tonerekke varsler også at prosessen var vellykket.
8. Ta ut disketten og slå på strømmen.
9. Slå på strømmen igjen for å starte maskinen på nytt.

Tabellen nedenfor viser de forskjellige tasturlampe-kombinasjonene som blir brukt av Boot Block ROM (når et PS/2-tastatur er koblet til datamaskinen), og forklarer betydningen og hva du skal gjøre.

Tastaturlampe-kombinasjoner som brukes av Boot Block ROM

FailSafe Boot Block-modus	Farge på tastatur-LED	Tastatur LED-aktivitet	Tilstand/Melding
Num Lock	Grønn	På	ROMPaq-diskett står ikke i, er skadet eller stasjonen er ikke klar.
Caps Lock	Grønn	På	Skriv passord.
Num, Caps, Scroll Lock	Grønn	Blink på i sekvens, en om gangen – N, C, SL	Tastatur låst i nettverksmodus.
Num, Caps, Scroll Lock	Grønn	På	Omprogrammering av oppstartsblokk-ROM var vellykket. Slå av strømmen og slå den på igjen for å starte på nytt.

 Diagnoselysene blinker ikke på USB-tastaturer.

Kopiere Setup

Denne prosedyren gjør at administratoren enkelt kan kopiere en konfigurasjon over til andre datamaskiner av samme modell. Dette gir raskere og mer konsekvent konfigurering for flere datamaskiner.



Begge prosedyrene krever en diskettstasjon eller en støttet USB Flash Media-enhet, for eksempel en HP Drive Key.

Kopiere til én datamaskin



FORSIKTIG! En setup-konfigurasjon er modellspesifikk. Filsystemet kan bli ødelagt hvis kilde- og måldatamaskinen ikke er av samme modell. Du må for eksempel ikke kopiere setup-konfigurasjonen fra en D510 Ultra-slim Desktop til en D510 e-pc.

1. Velg en setup-konfigurasjon som skal kopieres. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
 2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.
-



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Sett inn en diskett eller en USB Flash Media-enhet.
4. Velg **File > Save to Diskette**. Følg instruksjonene på skjermen for å opprette konfigurasjonsdisketten eller USB Flash Media-enheten.
5. Slå av datamaskinen som skal konfigureres, og sett inn konfigurasjonsdisketten eller USB Flash Media-enheten.
6. Slå på datamaskinen som skal konfigureres. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.
7. Velg **File > Restore from Diskette** og følg instruksjonene på skjermen.
8. Start datamaskinen på nytt når konfigurasjonen er fullført.

Kopiere til flere datamaskiner



FORSIKTIG! En setup-konfigurasjon er modellspesifikk. Filsystemet kan bli ødelagt hvis kilde- og måldatamaskinen ikke er av samme modell. Du må for eksempel ikke kopiere setup-konfigurasjonen fra en D510 Ultra-slim Desktop til en D510 e-pc.

Med denne metoden tar det litt lenger tid å klargjøre konfigurasjons-disketten eller USB Flash Media-enheten, men selve kopieringen av konfigurasjonen til målmaskinene tar mye kortere tid.



En oppstartbar diskett kan ikke opprettes i Windows 2000. Det kreves en oppstartbar diskett for denne prosedyren eller for å opprette en oppstartbar USB Flash Media-enhet. Hvis Windows 9x eller Windows XP ikke er tilgjengelig for å opprette en oppstartbar diskett, bruker du metoden for å kopiere til én datamaskin isteden (se ["Kopiere til én datamaskin" på side 10](#)).

1. Opprett en oppstartbar diskett eller USB Flash Media-enhet. Se ["Oppstartbar diskett" på side 12](#), ["USB Flash Media-enhet som støttes" på side 13](#) eller ["USB Flash Media-enhet som ikke støttes" på side 16](#).



FORSIKTIG! Ikke alle datamaskiner kan starte opp fra en USB Flash Media-enhet. Hvis standard oppstartrekkefølge i Computer Setup (F10) angir USB-enheten før harddisken, kan datamaskinen startes opp fra en USB Flash Media-enhet. Hvis ikke, må det brukes en oppstartbar diskett.

2. Velg en setup-konfigurasjon som skal kopieres. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
3. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

4. Sett inn den oppstartbare disketten eller USB Flash Media-enheten.
5. Velg **File > Save to Diskette**. Følg instruksjonene på skjermen for å opprette konfigurasjonsdisketten eller USB Flash Media-enheten.
6. Last ned et BIOS-hjelpeprogram for å kopiere setup (repset.exe), og kopier det til konfigurasjonsdisketten eller USB Flash Media-enheten. Du finner hjelpeprogrammet på <http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html>.
7. På konfigurasjonsdisketten eller USB Flash Media-enheten oppretter du en autoexec.bat-fil som inneholder følgende kommando:
repset.exe
8. Slå av datamaskinen som skal konfigureres. Sett inn konfigurasjonsdisketten eller USB Flash Media-enheten og slå på datamaskinen. Konfigurasjonshjelpeprogrammet kjører automatisk.
9. Start datamaskinen på nytt når konfigurasjonen er fullført.

Opprette en oppstartbar enhet

Oppstartbar diskett



Disse instruksjonene er for Windows XP Professional og Home Edition. Windows 2000 støtter ikke opprettelse av oppstartbare disketter.

1. Sett inn en diskett i diskettstasjonen.
2. Klikk **Start**, og deretter **Min datamaskin**.
3. Høyreklikk stasjonsbokstaven og klikk **Formater**.
4. Velg **Gjør dette til en oppstartsdiskett for MS-DOS**, og klikk **Start**.

Gå tilbake til "[Kopiere til flere datamaskiner](#)" på side 11.

USB Flash Media-enhet som støttes

Enheter som støttes, for eksempel en HP Drive Key eller en DiskOnKey, har et forhåndsinstallert bilde for å forenkle prosessen med å gjøre dem opstartbare. Hvis den Drive Key som støttes, ikke har dette bildet, bruker du prosedyren lenger ute i dette kapittelet (se ["USB Flash Media-enhet som ikke støttes" på side 16](#)).



FORSIKTIG! Ikke alle datamaskiner kan starte opp fra en USB Flash Media-enhet. Hvis standard oppstartrekkefølge i Computer Setup (F10) angir USB-enheten før harddisken, kan datamaskinen startes opp fra en USB Flash Media-enhet. Hvis ikke, må det brukes en oppstartbar diskett.

For å opprette en oppstartbar USB Flash Media-enhet må du ha:

■ Ett av følgende systemer:

- ☐ Compaq Evo D510 Ultra-slim Desktop
- ☐ Compaq Evo D510 Convertible Minitower/Small Form Factor
- ☐ HP Compaq Business Desktop d530 Series – Ultra-slim Desktop, Small Form Factor eller Convertible Minitower
- ☐ Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c eller N1000c Notebooks
- ☐ Compaq Presario 1500 eller 2800 Notebooks

Avhengig av den enkelte BIOS kan fremtidige systemer også støtte oppstart til HP Drive Key.



FORSIKTIG! Hvis du bruker en annen datamaskin enn det som er nevnt over, må du kontrollere at standard oppstartsrekkefølge i Computer Setup (F10) angir USB-enheten før harddisken.

■ En av følgende lagringsmoduler:

- ☐ 16 MB HP Drive Key
- ☐ 32 MB HP Drive Key
- ☐ 32 MB DiskOnKey
- ☐ 64 MB HP Drive Key
- ☐ 64 MB DiskOnKey
- ☐ 128 MB HP Drive Key
- ☐ 128 MB DiskOnKey

- En oppstartbar DOS-diskett med FDISK- og SYS-programmene. Hvis SYS ikke er tilgjengelig, kan FORMAT brukes, men alle eksisterende filer på Drive Key vil gå tapt.
1. Slå av datamaskinen.
 2. Sett inn Drive Key i en av USB-portene på datamaskinen, og fjern alle andre USB-lagringenheter, bortsett fra USB-diskettstasjoner.
 3. Sett inn en oppstartbar DOS-diskett med FDISK.COM og enten SYS.COM eller FORMAT.COM i en diskettstasjon, og slå på datamaskinen for å starte opp til DOS-disketten.
 4. Kjør FDISK fra A:\ ved å skrive **FDISK** og trykke på Enter. Hvis du blir bedt om det, klikker du **Yes (Y)** for å aktivere støtte for stor disk.
 5. Angi valget [**5**] for å vise stasjonene i systemet. Drive Key vil være stasjonen som samsvarer nært med størrelsen på en av de angitte stasjonene. Det vil vanligvis være den siste stasjonen på listen. Noter deg stasjonsbokstaven.

Drive Key-stasjon: _____



FORSIKTIG! Hvis en stasjon ikke samsvarer med Drive Key, må du ikke fortsette. Du kan miste data. Kontroller alle USB-porter for andre lagringenheter. Hvis du finner andre, fjerner du dem, starter maskinen på nytt og fortsetter fra trinn 4. Hvis du ikke finner noen, støtter ikke systemet Drive Key eller Drive Key er defekt. IKKE fortsett med å forsøke å gjøre Drive Key oppstartbar.

6. Avslutt FDISK ved å trykke **Esc**-tasten for å gå tilbake til ledeteksten A:\.
7. Hvis den oppstartbare DOS-disketten inneholder SYS.COM, går du til trinn 8. Hvis ikke, går du til trinn 9.
8. Ved ledeteksten A:\ skriver du **SYS x:** der x er stasjonsbokstaven du noterte over. Gå til trinn 13.



FORSIKTIG! Kontroller at du har angitt riktig stasjonsbokstav for Drive Key.

Når systemfilene er overført, vil SYS gå tilbake til A:\.

9. Kopier eventuelle filer du vil beholde, fra Drive Key til en midlertidig katalog på en annen stasjon (for eksempel systemets interne harddisk).
10. Ved ledeteksten A:\ skriver du **FORMAT /S X:** der x er stasjonsbokstaven du noterte over.



FORSIKTIG! Kontroller at du har angitt riktig stasjonsbokstav for Drive Key.

FORMAT vil vise en eller flere advarsler og spør deg hver gang om du vil fortsette. Angi **y** hver gang. FORMAT vil formatere Drive Key, legge til systemfiler og be om en volumetikett.

11. Trykk **Enter** for ingen etikett eller angi en.
12. Kopier eventuelle filer du lagret i trinn 9, tilbake til Drive Key.
13. Ta ut disketten og start maskinen på nytt. Datamaskinen vil starte opp til Drive Key som stasjon C.



Standard oppstartsrekkefølge varierer fra datamaskin til datamaskin, og kan endres i Computer Setup (F10).

Hvis du har brukt en DOS-versjon fra Windows 9x, er det mulig at du ser en kort Windows-logoskjerm. Hvis du ikke ønsker denne skjermen, legger du til en null-lengdes fil kalt LOGO.SYS til rotkatalogen for Drive Key.

Gå tilbake til ["Kopiere til flere datamaskiner"](#) på side 11.

USB Flash Media-enhet som ikke støttes



FORSIKTIG! Ikke alle datamaskiner kan starte opp fra en USB Flash Media-enhet. Hvis standard oppstartrekkefølge i Computer Setup (F10) angir USB-enheten før harddisken, kan datamaskinen startes opp fra en USB Flash Media-enhet. Hvis ikke, må det brukes en oppstartbar diskett.

For å opprette en oppstartbar USB Flash Media-enhet må du ha:

- Ett av følgende systemer:
 - ☐ Compaq Evo D510 Ultra-slim Desktop
 - ☐ Compaq Evo D510 Convertible Minitower/Small Form Factor
 - ☐ HP Compaq Business Desktop d530 Series – Ultra-slim Desktop, Small Form Factor eller Convertible Minitower
 - ☐ Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c eller N1000c Notebooks
 - ☐ Compaq Presario 1500 eller 2800 Notebooks

Avhengig av den enkelte BIOS kan fremtidige systemer også støtte oppstart til en USB Flash Media-enhet.



FORSIKTIG! Hvis du bruker en annen datamaskin enn det som er nevnt over, må du kontrollere at standard oppstartsrekkefølge i Computer Setup (F10) angir USB-enheten før harddisken.

- En oppstartbar DOS-diskett med FDISK- og SYS-programmene. Hvis SYS ikke er tilgjengelig, kan FORMAT brukes, men alle eksisterende filer på Drive Key vil gå tapt.
 1. Hvis systemet har PCI-kort som har SCSI-, ATA RAID- eller SATA-stasjoner tilkoblet, slår du av datamaskinen og trekker du strømledningen.
-



FORSIKTIG! Strømledningen MÅ være koblet fra.

2. Åpne datamaskinen og ta ut PCI-kortene.
3. Sett inn USB Flash Media-enheten i en av USB-portene på datamaskinen, og fjern alle andre USB-lagringenheter, bortsett fra USB-diskettstasjoner. Lukk maskindekselet.

4. Plugg inn strømledningen og slå på datamaskinen. Når lampen på skjermen lyser grønt, trykker du **F10**-tasten for å gå inn i hjelpeprogrammet Computer Setup.
5. Gå til Advanced/PCI devices for å deaktivere både IDE- og SATA-kontrollere. Når du deaktiverer SATA-kontrolleren, noterer du IRQen som kontrolleren er tilordnet. Du må tilordne IRQ på nytt senere. Avslutt Setup, bekreft endringene.
IRQ FOR SATA: _____
6. Sett inn en oppstartbar DOS-diskett med FDISK.COM og enten SYS.COM eller FORMAT.COM i en diskettstasjon, og slå på datamaskinen for å starte opp til DOS-disketten.
7. Kjør FDISK og slett eventuelle eksisterende partisjoner på USB Flash Media-enheten. Lag en ny partisjon og merk den som aktiv. Avslutt FDISK ved å trykke **Esc**-tasten.
8. Hvis systemet ikke startet opp på nytt automatisk da du avsluttet FDISK, trykker du **Ctrl+Alt+Del** for å starte opp til DOS-disketten.
9. Ved ledeteksten A:\ skriver du **FORMAT C: /S** og trykker **Enter**. FORMAT vil formatere USB Flash Media-enheten, legge til systemfiler og be om en volumetikett.
10. Trykk **Enter** for ingen etikett eller angi en.
11. Slå av datamaskinen og trekk ut strømledningen. Åpne datamaskinen og reinstaller eventuelle PCI-kort du har fjernet. Lukk maskindekselet.
12. Plugg inn strømledningen, fjern disketten og slå på datamaskinen.
13. Når lampen på skjermen lyser grønt, trykker du **F10**-tasten for å gå inn i hjelpeprogrammet Computer Setup.
14. Gå til Advanced/PCI Devices og reaktiver IDE- og SATA-kontrollerne du deaktiverte i trinn 5. Plasser SATA-kontrolleren i dens opprinnelige IRQ.
15. Lagre endringene og avslutt Datamaskinen vil starte opp til USB Flash Media-enheten som stasjon C.



Standard oppstartsrekkefølge varierer fra datamaskin til datamaskin, og kan endres i Computer Setup (F10).

Hvis du har brukt en DOS-versjon fra Windows 9x, er det mulig at du ser en kort Windows-logoskjerm. Hvis du ikke ønsker denne skjermen, legger du til en null-lengdes fil kalt LOGO.SYS til rotkatalogen for Drive Key.

Gå tilbake til ["Kopiere til flere datamaskiner"](#) på side 11.

Strømbryter med dobbelt funksjon

Med ACPI (Advanced Configuration and Power Interface) aktivert for Windows 2000 og Windows XP Professional og Home Edition kan strømbryteren fungere enten som av/på-bryter eller som hvilemodusknapp. Hvilemodus-funksjonen slår ikke strømmen helt av, men gjør at datamaskinen går inn i en hviletilstand med lavt strømforbruk. Dette gjør at du kan slå av maskinen raskt uten å lukke programmer, og gå raskt tilbake til samme bruksstatus uten å miste data.

Slik endrer du konfigurasjonen for strømbryteren:

1. I Windows 2000 venstreklikker du på **Start-knappen** og deretter velger du **Innstillinger > Kontrollpanel > Strømalternativer**.
I Windows XP Professional og Home Edition venstreklikker du på **Start-knappen**, og velg deretter **Kontrollpanel > Ytelse og vedlikehold > Strømalternativer**.
2. I **Egenskaper for Strømalternativer** velger du kategorien **Avansert**.
3. Under **Av/på-knapper** velger du ønsket innstilling for strømbryteren.

Når du har konfigurert strømbryteren slik at den fungerer som en hvilemodusknapp, trykker du på strømbryteren for å sette maskinen i en tilstand med lavt strømforbruk (hvilemodus). Trykk på knappen en gang til for å få maskinen raskt ut av hvilemodus og tilbake til fullt strømforbruk. Hvis du vil slå all strøm til systemet helt av, må du trykke og holde inne strømbryteren i fire sekunder.



FORSIKTIG! Ikke bruk strømbryteren til å slå av datamaskinen med mindre systemet ikke reagerer. Hvis du slår av strømmen uten å avslutte operativsystemet, kan det føre til skade på eller tap av data på harddisken.

Nettsted

HP-teknikerne utfører omfattende testing og feilsøking av programvare som er utviklet av HP og tredjepartsleverandører, for å sikre best mulig ytelse, kompatibilitet og pålitelighet for HP-PCer.

Når du går over til nye eller endrede operativsystemer, er det viktig å implementere støtteprogramvaren som er utviklet for det aktuelle operativsystemet. Hvis du har tenkt å kjøre en versjon av Microsoft Windows som er forskjellig fra versjonen som følger med datamaskinen, må du installere tilsvarende enhetsdrivere og verktøy for å sikre at alle funksjonene er støttet og fungerer som de skal.

HP har gjort det lettere å finne, få tilgang til, vurdere og installere den nyeste støtteprogramvaren. Du kan laste ned programvaren fra <http://www.hp.com/support>.

Nettstedet inneholder de nyeste nettverksdriverne, verktøy og omprogrammerbare ROM-bilder som er nødvendige for å kjøre det nyeste Microsoft Windows-operativsystemet på din HP-datamaskin.

Byggeklusser og partnere

HP administrasjonsløsninger integreres med andre systemadministrasjonsprogrammer, og er basert på bransjestandarder, for eksempel:

- Desktop Management Interface (DMI) 2.0
- Wake on LAN-teknologi
- ACPI
- SMBIOS
- Støtte for Pre-boot Execution (PXE)

Aktivasporing og sikkerhet

Aktivasporingsfunksjonene som er bygd inn i datamaskinen, gir viktige aktivasporingsdata som kan behandles ved hjelp av HP Insight Manager, HP Client Manager og andre systemadministrasjonsprogrammer. Veltilpasset, automatisk integrasjon mellom aktivasporingsfunksjonene og disse produktene gjør at du kan velge det behandlingsverktøyet som passer best for ditt arbeidsmiljø, og dra nytte av dine investeringer i eksisterende verktøy.

HP tilbyr også flere løsninger for kontroll over tilgangen til verdifulle komponenter og informasjon. Hvis ProtectTools Embedded Security er installert, hindrer dette uautorisert tilgang til data, det kontrollerer systemintegriteten og autentifiserer tredjepartsbrukere som forsøker å få tilgang til systemet. Sikkerhetsfunksjoner som ProtectTools, Smart dekselsensor og Smart deksellås, som finnes på enkelte modeller, bidrar til å forhindre uautorisert tilgang til datamaskinens interne komponenter. Hvis du deaktiverer parallelle porter, serielle porter eller USB-porter, eller hvis du deaktiverer funksjonen for oppstart fra uttagbart medium, kan du beskytte verdifulle dataaktiva. Varsler fra Minneendring og Smart dekselsensor kan videresendes automatisk til systemadministrasjonsprogrammer for å gi proaktiv varsling om klussing med en datamaskins interne komponenter.




ProtectTools, Smart dekselsensor og Smart deksellås er tilgjengelige som alternativer på enkelte systemer.

Bruk følgende verktøy til å behandle sikkerhetsinnstillinger i HP-datamaskinen:


- Lokalt, ved hjelp av verktøy for maskininstallasjon (Computer Setup Utilities). Se *Computer Setup (F10) Utility Guide* som følger med datamaskinen for ytterligere informasjon og anvisninger om bruken av Computer Setup-verktøyet.
- Fjernstyrt, med bruk av HP Client Manager eller System Software Manager. Denne programvaren gir sikker, konsekvent distribusjon av og kontroll med sikkerhetsinnstillinger fra et enkelt kommandolinjeverktøy.

Tabellen og delene nedenfor henviser til funksjoner for sikkerhetsbehandling på datamaskinen lokalt ved hjelp av verktøy for maskinoppsett (Computer Setup Utilities – F10).


Oversikt over sikkerhetsfunksjoner

Funksjon	Formål	Hvordan den etableres
Uttagbar media oppstartskontroll	Hindrer oppstart fra stasjoner for uttagbare medier. (tilgjengelig på visse stasjoner)	Fra Computer Setup (F10) Utilities-menyen.
Seriell, parallell, USB eller infrarød grensesnittkontroll	Hindrer overføring av data gjennom det serielle, parallell, USB- (universal serial bus) eller infrarøde grensesnittet.	Fra Computer Setup (F10) Utilities-menyen.
Passord ved oppstart	Hindrer at datamaskinen brukes før passordet er oppgitt. Det kan gjelde både ved første oppstart og når maskinen startes på nytt.	Fra Computer Setup (F10) Utilities-menyen.
Konfigureringspassord	Hindrer omkonfigurering av datamaskinen (bruk av hjelpeprogrammet Computer Setup) før passordet er angitt.	Fra Computer Setup (F10) Utilities-menyen.
Innebygd sikkerhetsenhet	Hindrer uautorisert tilgang til data ved hjelp av kryptering og passordbeskyttelse. Kontrollerer systemintegriteten og autentifiserer tredjepartsbrukere som prøver å få tilgang til systemet.	Fra Computer Setup (F10) Utilities-menyen.
DriveLock	Hindrer uautorisert tilgang til data på MultiBay-harddisker. Denne funksjonen er tilgjengelig kun på enkelte modeller.	Fra Computer Setup (F10) Utilities-menyen.
 Se i håndboken <i>Computer Setup (F10) Utility Guide</i> for å få mer informasjon om Computer Setup. Støtte for sikkerhetsfunksjonene kan variere avhengig av datamaskinkonfigurasjonen.		

Oversikt over sikkerhetsfunksjoner (Fortsetter)

Funksjon	Formål	Hvordan den etableres
Smart dekselsensor	Indikerer at datamaskindekslet eller sidepanelet er fjernet. Den kan angis slik at konfigureringspassordet må skrives inn før datamaskinen kan startes på nytt, etter at dekslet eller sidepanelet er fjernet. Se håndboken <i>Hardware Reference Guide</i> på CDen <i>Compaq Reference Library</i> for mer informasjon om denne funksjonen. Denne funksjonen er tilgjengelig kun på enkelte modeller.	Fra Computer Setup (F10) Utilities-menyen.
Master Boot Record-sikkerhet	Kan forhindre utilsiktede eller ondsinnede forandringer i den gjeldende oppstartbare diskens Master Boot Record, og fungerer som et middel til gjenoppretting av den "sist kjente, gode" MBR.	Fra Computer Setup (F10) Utilities-menyen.
Minneendringsvarsler	Registrerer når minnemoduler er blitt lagt til, flyttet eller fjernet; varsler bruker og systemansvarlig.	Hvis du vil ha informasjon om hvordan du aktiverer varsel om minneendring, se den elektroniske håndboken <i>Intelligent Manageability Guide</i> .
 Se i håndboken <i>Computer Setup (F10) Utility Guide</i> for å få mer informasjon om Computer Setup. Støtte for sikkerhetsfunksjonene kan variere avhengig av datamaskinkonfigurasjonen.		

Oversikt over sikkerhetsfunksjoner (Fortsetter)

Funksjon	Formål	Hvordan den etableres
Eierinformasjon	Viser informasjon om eierskap, slik den er definert av systemadministratoren, under systemkonfigurerings (beskyttet av konfigureringspassord).	Fra Computer Setup (F10) Utilities-menyen.
Kabellåsutstyr	Gjør det vanskelig å komme til innsiden av datamaskinen, slik at du lettere unngår uønskede endringer i konfigurasjonen eller fjerning av komponenter. Kan også brukes til å feste datamaskinen til en fast gjenstand for å forhindre tyveri.	Installer en kabellås for å feste datamaskinen til en fastmontert gjenstand.
Sikkerhetssløyfeutstyr	Gjør det vanskelig å komme til innsiden av datamaskinen, slik at du lettere unngår uønskede endringer i konfigurasjonen eller fjerning av komponenter.	Installer en lås i sikkerhetssløyfen for å forhindre uønskede endringer i konfigurasjonen eller fjerning av komponenter.
 Se i håndboken <i>Computer Setup (F10) Utility Guide</i> for å få mer informasjon om Computer Setup. Støtte for sikkerhetsfunksjonene kan variere avhengig av datamaskinkonfigurasjonen.		

Passordsikkerhet

Oppstartspassordet forhindrer uautorisert bruk av datamaskinen, ved å kreve passord for å få tilgang til programmer eller data hver gang maskinen blir slått på eller startes på nytt. Konfigurasjonspassordet forhindrer spesielt uautorisert tilgang til Computer Setup, og kan også brukes til å overstyre oppstartspassordet. Det vil si at når du blir bedt om å oppgi oppstartspassordet, vil du få tilgang til datamaskinen ved å oppgi konfigurasjonspassordet.

Det kan opprettes et konfigureringspassord for hele nettverket, slik at systemansvarlig kan logge på alle nettverksmaskiner for å utføre vedlikehold, uten at det er nødvendig å vite oppstartspassordet, selv om det finnes et slikt passord.

Etablere et konfigureringspassord ved hjelp av Computer Setup

Hvis systemet er utstyrt med en innebygd sikkerhetsenhet, kan du se ["Innebygd sikkerhet" på side 29](#).

Ved å opprette et konfigureringspassord i Computer Setup hindrer du omkonfigurering av datamaskinen (bruk av hjelpeprogrammet Computer Setup) før passordet angis.

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Velg **Security**, og velg deretter **Setup Password** og følg anvisningene på skjermen.
4. Før du avslutter, klikker du på **File > Save Changes** og **Exit**.

Opprette et oppstartspassord ved hjelp av Computer Setup

Hvis du etablerer et oppstartspassord med Computer Setup kan ingen få tilgang til datamaskinen når strømmen er slått på, med mindre passordet blir oppgitt. Når et oppstartspassord er etablert, vil Computer Setup vise Password Options under Security-menyen. Password options (Passordalternativer) omfatter Password Prompt on Warm Boot (Anmodning om passord ved varmstart). Også når Anmodning om passord ved varmstart aktivert, må passordet tastes inn hver gang datamaskinen startes på nytt.

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Velg **Security** og deretter **Power-On Password** og følg anvisningene på skjermen.
4. Før du avslutter, klikker du på **File > Save Changes og Exit**.

Angi et oppstartspassord

Slik angir du et oppstartspassord:

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
2. Når nøkkelikonet vises på skjermen, skriver du inn det gjeldende passordet og trykker på **Enter**.



Vær omhyggelig når du skriver; av sikkerhetsgrunner vil ikke tegnene du skriver, bli vist på skjermen.

Hvis du skriver passordet feil, vil det komme frem et ikon med en brukket nøkkel. Prøv igjen. Hvis du ikke får det til på tre forsøk, må du slå datamaskinen av og på igjen før du kan fortsette.

Angi et konfigurasjonspassord

Hvis systemet er utstyrt med en innebygd sikkerhetsenhet, kan du se ["Innebygd sikkerhet" på side 29](#).

Hvis et konfigurasjonspassord er opprettet på Internett-enheten, vil du bli bedt om å angi det hver gang du kjører Computer Setup.

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Når nøkkelikonet vises på skjermen, skriver du inn konfigureringspassordet og trykker **Enter**.



Vær omhyggelig når du skriver; av sikkerhetsgrunner vil ikke tegnene du skriver, bli vist på skjermen.

Hvis du skriver passordet feil, vil det komme frem et ikon med en brukket nøkkel. Prøv igjen. Hvis du ikke får det til på tre forsøk, må du slå datamaskinen av og på igjen før du kan fortsette.

Endre et oppstarts- eller konfigureringspassord

Hvis systemet er utstyrt med en innebygd sikkerhetsenhet, kan du se ["Innebygd sikkerhet" på side 29](#).

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**. Hvis du vil endre konfigureringspassordet, kjører du **Computer Setup**.
2. Når nøkkelikonet vises, skriver du inn det gjeldende passordet, en skråstrek (/) eller et annet skilletegn, det nye passordet, en ny skråstrek (/) eller et annet skilletegn, og det nye passordet på nytt, som vist nedenfor:
nåværende passord/nytt passord/nytt passord



Vær omhyggelig når du skriver; av sikkerhetsgrunner vil ikke tegnene du skriver, bli vist på skjermen.

3. Trykk på **Enter**-tasten.

Det nye passordet trer i kraft neste gang du slår på datamaskinen.



Se "[Grensetegn for nasjonale tastatur](#)" på side 28 for informasjon om andre skilletegn. Oppstartspassordet og konfigurasjonspassordet kan også endres ved hjelp av alternativene i Security i Computer Setup.

Slette et oppstarts- eller konfigureringspassord

Hvis systemet er utstyrt med en innebygd sikkerhetsenhet, kan du se "[Innebygd sikkerhet](#)" på side 29.

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**. Hvis du vil slette konfigureringspassordet, kjører du **Computer Setup**.
 2. Når nøkkelikonet kommer frem, skriver du det gjeldende passordet og en skråstrek (/) eller alternativt skilletegn, som vist nedenfor:
gjeldende passord/
 3. Trykk på **Enter**-tasten.
-



Se "[Grensetegn for nasjonale tastatur](#)" for informasjon om andre skilletegn. Oppstartspassordet og konfigurasjonspassordet kan også endres ved hjelp av alternativene i Security i Computer Setup.

Grensetegn for nasjonale tastatur

Alle tastaturer er laget slik at de oppfyller kravene i et bestemt land. Syntaksen og tastene du bruker for å endre eller slette passordet, avhenger av tastaturet som ble levert med datamaskinen.

Grensetegn for nasjonale tastatur

Arabisk	/	Gresk	-	Russisk	/
Belgisk	=	Hebraisk	.	Slovakisk	-
BHCSY*	-	Ungarsk	-	Spanish	-
Portugisisk (Brasil)	/	Italian	-	Svensk/finsk	/
Kinesisk	/	Japanese	/	Sveitsisk	-
Tsjekkisk	-	Koreansk	/	Taiwansk	/
Dansk	-	Latinamerikansk	-	Thai	/
French	!	Norsk	-	Tyrkisk	.
Fransk (Canada)	é	Polsk	-	Engelsk (Storbritannia)	/
German	-	Portugisisk	-	Engelsk (USA)	/

* For Bosnia-Hercegovina, Kroatia, Slovenia og Jugoslavia

Fjerning av passord

Hvis du glemmer passordet, kan du ikke få tilgang til datamaskinen. Slå opp under *Feilsøking* hvis du vil vite mer om fjerning av passord.

Hvis systemet er utstyrt med en innebygd sikkerhetsenhet, kan du se ["Innebygd sikkerhet."](#)

Innebygd sikkerhet

ProtectTools Embedded Security kombinerer kryptering og passordbeskyttelse for å gi økt sikkerhet for fil-/mappekryptering for EFS (Embedded File System) og sikker e-post med Microsoft Outlook og Outlook Express. ProtectTools er tilgjengelig for utvalgte stasjonære forretnings-PCer som CTO-alternativer (Configured-To-Order). Det er beregnet for HP-kunder som mener at datasikkerhet er det viktigste av alt: uautorisert tilgang til data innebærer en langt større fare enn tap av data. ProtectTools bruker fire passord:

- (F10) Setup – for å gå inn i Computer Setup (F10) og aktivere/deaktivere ProtectTools
- Take Ownership – skal innstilles og brukes av en systemadministrator, som vil autorisere brukere og definere sikkerhetsparametere
- Emergency Recovery Token – skal innstilles av systemadministratoren, vil muliggjøre gjenoppretting ved feil med datamaskin eller ProtectTools-brikke
- Basic User – skal innstilles og brukes av sluttbrukeren



Hvis sluttbrukerens passord går tapt, kan de krypterte dataene ikke gjenopprettes. Derfor er bruken av ProtectTools tryggest når dataene på brukerens stasjon kopieres på et systeminformasjonssystem eller sikkerhetskopieres regelmessig.

ProtectTools Embedded Security er en TCPA 1.1-kompatibel sikkerhetsbrikke som kan installeres som ekstraustyr på systemkortet på utvalgte stasjonære forretnings-PCer. Hver ProtectTools Embedded Security-brikke er unik og er bundet til en bestemt datamaskin. Hver brikke utfører viktige sikkerhetsprosesser uavhengig av andre datamaskinkomponenter (for eksempel prosessor, minne eller operativsystem).

En ProtectTools Embedded Security-aktivert datamaskin kompletterer og utvider sikkerhetsegenskapene som er innebygd i Microsoft Windows 2000 eller Windows XP Professional eller Home Edition. Eksempel: Mens operativsystemet kan kryptere lokale filer og mapper basert på en EFS, tilbyr ProtectTools Embedded Security et ekstra sikkerhetslag ved å opprette krypteringsnøkler fra plattformens rotnøkkel (som er lagret i silikon). Prosessen kalles “wrapping” av krypteringsnøkler. ProtectTools hindrer ikke nettverkstilgang til en datamaskin uten ProtectTools.

Viktige egenskaper for ProtectTools Embedded Security omfatter:

- Plattformautentifisering
- Beskyttet lagring
- Dataintegritet



FORSIKTIG! Vern av passord. **Krypterte data kan ikke aksesserer eller gjenopprettes uten passord.**

Definere passord

Konfigurering

Et konfigureringspassord kan opprettes og den innebygde sikkerhetsenheten kan aktiveres med hjelpeprogrammet Computer Setup (F10).

1. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

2. Bruk piltastene (opp eller ned) til å velge språk, deretter trykker du på **Enter**.
3. Bruk piltastene (venstre eller høyre) til å flytte til kategorien **Security**, deretter bruker du opp- eller nedpilene til å gå til **Setup Password**. Trykk **Enter**.
4. Skriv inn og bekreft passordet. Trykk **F10** for å godta passordet.



Vær omhyggelig når du skriver; av sikkerhetsgrunner vil ikke tegnene du skriver, bli vist på skjermen.

5. Bruk piltastene (opp eller ned) til å gå til **Embedded Security Device**. Trykk **Enter**.

6. Hvis valget i dialogboksen er **Embedded Security Device – Disable**, bruker du venstre- eller høyrepilen til å endre det til **Embedded Security Device – Enable**. Trykk **F10** for å godta endringen.



FORSIKTIG! Hvis du velger **Reset to Factory Settings – Reset**, tømmer alle nøklene og krypterte data vil ikke kunne gjenopprettes *med mindre* det er tatt sikkerhetskopi av dem (se [“Take Ownership og Emergency Recovery Token”](#)). Du må bare velge **Reset** når du får beskjed om det i prosedyren for å gjenopprette krypterte data (se [“Gjenopprette krypterte data” på side 33](#)).

7. Bruk piltastene (venstre eller høyre) til å flytte til **File**. Bruk piltastene (opp eller ned) til å gå til **Save Changes and Exit**. Trykk **Enter**, og trykk deretter **F10** for å bekrefte.

Take Ownership og Emergency Recovery Token

Take Ownership-passordet er nødvendig for å aktivere eller deaktivere sikkerhetsplattformen og autorisere brukere. Hvis det er feil med den innebygde sikkerhetsenheten, vil gjenopprettingsmekanismen gjøre at brukere kan autoriseres og data aksesseres.

1. Hvis du bruker Windows XP Professional eller Home Edition, klikker du på **Start > Alle programmer > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

Hvis du bruker Windows 2000, klikker du på **Start > Programmer > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

2. Klikk **Next**.
3. Skriv inn og bekreft et Take Ownership-passord, og klikk **Next**.



Vær omhyggelig når du skriver; av sikkerhetsgrunner vil ikke tegnene du skriver, bli vist på skjermen.

4. Klikk **Next** for å godta standardplasseringen for gjenopprettingsarkivet.
5. Skriv inn og bekreft et Emergency Recovery Token-passord, og klikk **Next**.

6. Sett inn en diskett der Emergency Recovery Token-nøkkelen skal lagres. Klikk **Browse** og velg disketten.



FORSIKTIG! Emergency Recovery Token-nøkkelen brukes til å gjenopprette krypterte data ved feil på en datamaskin eller innebygd sikkerhetsbrikke. **Dataene kan ikke gjenopprettes uten nøkkelen.** (Krypterte data kan ikke aksesseres uten Basic User-passordet.) Lagre disketten på et trygt sted.

7. Klikk **Save** for å godta plasseringen og standardfilnavnet, og klikk **Next**.
8. Klikk **Next** for å bekrefte innstillingene før sikkerhetsplattformen initialiseres.



Det kan hende du får opp en melding om at den innebygde sikkerhetsfunksjonen ikke er initialisert. Ikke klikk i meldingen; den adresseres senere i prosedyren og lukkes etter noen få sekunder.

9. Klikk **Next** for å omgå konfigurering av lokale retningslinjer.
10. Kontroller at boksen Start Embedded Security User Initialization Wizard er valgt, og klikk **Finish**.

Veiviseren for brukerinitialisering starter automatisk.

Basic User

Under initialiseringen opprettes Basic User-passordet. Passordet er nødvendig for å angi og aksessere krypterte data.



FORSIKTIG! Beskytt Basic User-passordet. **Krypterte data kan ikke aksesseres eller gjenopprettes uten dette passordet.**

1. Hvis veiviseren for brukerinitialisering ikke er åpen:

Hvis du bruker Windows XP Professional eller Home Edition, klikker du på **Start > Alle programmer > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

Hvis du bruker Windows 2000, klikker du på **Start > Programmer > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

2. Klikk **Next**.

3. Skriv inn og bekreft et Basic User-passord, og klikk **Next**.



Vær omhyggelig når du skriver; av sikkerhetsgrunner vil ikke tegnene du skriver, bli vist på skjermen.

4. Klikk **Next** for å bekrefte innstillingene.

5. Velg ønsket sikkerhetsfunksjon, og klikk **Next**.

6. Klikk ønsket e-postklient for å velge den, og klikk **Next**.

7. Klikk **Next** for å bruke krypteringssertifikatet.

8. Klikk **Next** for å bekrefte innstillingene.

9. Klikk **Finish**.

10. Start datamaskinen på nytt.

Gjenopprette krypterte data

For å gjenopprette data etter utskiftning av ProtectTools-brikken, må du ha følgende:

- SPemRecToken.xml – Emergency Recovery Token-nøkkelen
- SPemRecArchive.xml – skjult mappe, standardplassering:
C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- ProtectTools-passord
 - ☐ Setup
 - ☐ Take Ownership
 - ☐ Emergency Recovery Token
 - ☐ Basic User

1. Start datamaskinen på nytt.

2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Tast inn konfigureringspassordet, og trykk på **Enter**.

4. Bruk piltastene (opp eller ned) til å velge språk, deretter trykker du på **Enter**.

5. Bruk piltastene (venstre eller høyre) til å flytte til kategorien **Security**, deretter bruker du opp- eller nedpilene til å gå til **Embedded Security Device**. Trykk **Enter**.
6. Hvis bare ett valg, **Embedded Security Device – Disable**, er tilgjengelig:
 - a. Bruk piltastene (venstre eller høyre) til å endre det til **Embedded Security Device – Enable**. Trykk **F10** for å godta endringen.
 - b. Bruk piltastene (venstre eller høyre) til å flytte til **File**. Bruk piltastene (opp eller ned) til å gå til **Save Changes and Exit**. Trykk **Enter**, og trykk deretter **F10** for å bekrefte.
 - c. Gå til trinn 1.

Hvis to valg er tilgjengelig, går du til trinn 7.

7. Bruk piltastene (opp eller ned) til å gå til **Reset to Factory Settings – Do Not Reset**. Trykk venstre- eller høyrepilen én gang.

Det vises en melding som sier: Performing this action will reset the embedded security device to factory settings if settings are saved on exit. Press any key to continue.

Trykk **Enter**.

8. Valget vil nå være **Reset to Factory Settings – Reset**. Trykk **F10** for å godta endringen.
9. Bruk piltastene (venstre eller høyre) til å flytte til **File**. Bruk piltastene (opp eller ned) til å gå til **Save Changes and Exit**. Trykk **Enter**, og trykk deretter **F10** for å bekrefte.
10. Start datamaskinen på nytt.
11. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

12. Tast inn konfigureringspassordet, og trykk på **Enter**.
13. Bruk piltastene (opp eller ned) til å velge språk, deretter trykker du på **Enter**.

14. Bruk piltastene (venstre eller høyre) til å flytte til kategorien **Security**, deretter bruker du opp- eller nedpilene til å gå til **Embedded Security Device**. Trykk **Enter**.
15. Hvis valget i dialogboksen er **Embedded Security Device – Disable**, bruker du venstre- eller høyrepilen til å endre det til **Embedded Security Device – Enable**. Trykk **F10**.
16. Bruk piltastene (venstre eller høyre) til å flytte til **File**. Bruk piltastene (opp eller ned) til å gå til **Save Changes and Exit**. Trykk **Enter**, og trykk deretter **F10** for å bekrefte.
17. Etter at Windows er åpnet:

Hvis du bruker Windows XP Professional eller Home Edition, klikker du på **Start > Alle programmer > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

Hvis du bruker Windows 2000, klikker du på **Start > Programmer > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.
18. Klikk **Next**.
19. Skriv inn og bekreft Take Ownership-passordet. Klikk **Next**.



Vær omhyggelig når du skriver; av sikkerhetsgrunner vil ikke tegnene du skriver, bli vist på skjermen.

20. Kontroller at Create a new recovery archive er valgt. Under **Recovery archive location** klikker du **Browse**.
21. Ikke godta standardfilnavnet. Skriv inn et nytt filnavn for å unngå å erstatte den opprinnelige filen.
22. Klikk **Save**, og deretter **Next**.
23. Skriv inn og bekreft et Emergency Recovery Token-passord, og klikk **Next**.
24. Sett inn en diskett der Emergency Recovery Token-nøkkelen skal lagres. Klikk **Browse** og velg disketten.
25. Ikke godta standardnøkkelnavnet. Skriv inn et nytt nøkkelnavn for å unngå å erstatte den opprinnelige nøkkelen.
26. Klikk **Save**, og deretter **Next**.

27. Klikk **Next** for å bekrefte innstillingene før sikkerhetsplattformen initialiseres.



Det kan hende du får opp en melding som sier at Basic User-nøkkelen ikke kan lastes. Ikke klikk i meldingen; den adresseres senere i prosedyren og lukkes etter noen få sekunder.

28. Klikk **Next** for å omgå konfigurering av lokale retningslinjer.
29. Klikk for å fjerne avmerkingen i boksen **Start Embedded Security User Initialization Wizard**. Klikk **Finish**.
30. Høyreklikk ProtectTools-ikonet på verktøylinjen, og klikk **Initialize Embedded Security restoration**.
- Dette vil starte veiviseren for initialisering av HP ProtectTools Embedded Security.
31. Klikk **Next**.
32. Sett inn disketten der den opprinnelige Emergency Recovery Token-nøkkelen er lagret. Klikk **Browse**, finn plasseringen til og dobbeltklikk på tokenen for å angi navnet i feltet. Standarden er A:\SPEmRecToken.xml.
33. Skriv inn det opprinnelige Token-passordet, og klikk **Next**.
34. Klikk **Browse**, finn plasseringen til og dobbeltklikk det opprinnelige gjenopprettingsarkivet for å angi navnet i feltet. Standarden er C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Klikk **Next**.
36. Klikk maskinen som skal gjenopprettes, og klikk **Next**.
37. Klikk **Next** for å bekrefte innstillingene.
38. Hvis veiviseren sier at sikkerhetsplattformen er gjenopprettet, går du til trinn 39.
- Hvis veiviseren sier at gjenopprettingen er mislykket, går du tilbake til trinn 10. Kontroller passordene, tokenplassering og -navn og arkivplassering og -navn nøye.
39. Klikk **Finish**.

40. Hvis du bruker Windows XP Professional eller Home Edition, klikker du på **Start > Alle programmer > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

Hvis du bruker Windows 2000, klikker du på **Start > Programmer > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

41. Klikk **Next**.
42. Klikk **Recover your basic user key**, og klikk **Next**.
43. Velg en bruker, skriv inn det opprinnelige Basic User Key-passordet for brukeren, og klikk **Next**.
44. Klikk **Next** for å bekrefte innstillingene og godta standardplasseringen for gjenopprettingsdata.



Trinn 45 til 49 reinstallerer den opprinnelige Basic User-konfigurasjonen.

45. Velg ønsket sikkerhetsfunksjon, og klikk **Next**.
46. Klikk ønsket e-postklient for å velge den, og klikk **Next**.
47. Klikk krypteringssertifikatet, og klikk **Next** for å bruke det.
48. Klikk **Next** for å bekrefte innstillingene.
49. Klikk **Finish**.
50. Start datamaskinen på nytt.



FORSIKTIG! Beskytt Basic User-passordet. **Krypterte data kan ikke aksesseres eller gjenoprettes uten dette passordet.**

DriveLock

DriveLock er en bransjestandard sikkerhetsfunksjon som forhindrer uautorisert tilgang til data på MultiBay-harddisker. DriveLock er implementert som en utvidelse av Computer Setup. Det er bare tilgjengelig når DriveLock-kompatible harddisker er oppdaget.

DriveLock er beregnet for HP-kunder som mener at datasikkerhet er det viktigste av alt. For slike kunder er prisen på en harddisk og tapet av dataene som er lagret på den, av liten betydning i forhold til den skade som kunne oppstå hvis uvedkommende fikk tilgang til disse dataene. For å avbalansere dette sikkerhetsnivået med det praktiske behovet for å være behjelpelig med et glemt passord, bruker HPs implementering av DriveLock en sikkerhetsplan med to passord. Det ene passordet skal etableres og brukes av en systemansvarlig, mens det andre vanligvis etableres og brukes av sluttbrukeren. Det finnes ingen “bakdør” eller utvei som kan brukes til å låse opp harddisken hvis begge passordene blir mistet. Derfor er bruken av DriveLock tryggest når dataene på harddisken er replikert på en firmabasert informasjonssystem, eller sikkerhetskopieres regelmessig.

Hvis begge DriveLock-passordene skulle gå tapt, blir harddisken ubrukt. For brukere som ikke passer inn i den ovenfor definerte kundeprofilen, kan dette være en uakseptabel risiko. For brukere som passer inn i denne kundeprofilen, kan det være en akseptabel risiko med tanke på arten av dataene som er lagret på harddisken.

Bruke DriveLock

DriveLock-alternativet vises under Security-menyen i Computer Setup. Brukeren står overfor valget mellom å etablere et master-passord eller å aktivere DriveLock. Det må angis et brukerpasord for å aktivere DriveLock. Siden den første konfigureringen av DriveLock vanligvis foretas av en systemansvarlig, må master-passordet etableres først. HP oppfordrer systemansvarlige til å etablere et master-passord enten de har tenkt å aktivere DriveLock eller beholde den deaktivert. Dette gir den systemansvarlige mulighet til å endre DriveLock-innstillingene hvis disken låses i fremtiden. Så snart master-passordet er etablert, kan system systemansvarlige aktivere DriveLock eller velge å beholde den deaktivert.

Hvis det finnes en låst harddisk, vil POST kreve et passord for å låse opp enheten. Hvis det er etablert et oppstartspassord, og det passer til enhetens brukerpasord, vil ikke POST be brukeren om å angi passordet en gang til. Ellers blir brukeren bedt om å angi et DriveLock-passord. Enten master-passordet eller brukerpasordet kan brukes. Brukeren blir tildelt to forsøk på å skrive inn riktig passord. Hvis ingen av forsøkene lykkes, vil POST fortsette, men disken vil være utilgjengelig.

DriveLock-programmer

Den mest praktiske bruken av sikkerhetsfunksjonen DriveLock er i et konsernmiljø der en systemansvarlig forsyner brukerne med MultiBay-harddisker for bruk i noen datamaskiner. Den systemansvarlige skal ha ansvaret for konfigureringen av MultiBay-harddisken, som blant annet medfører etablering av master-passordet for DriveLock. Hvis brukeren skulle glemme brukerpasordet eller utstyret overføres til en annen ansatt, kan master-passordet alltid brukes til å etablere brukerpasordet på nytt og få tilgang til harddisken.

HP anbefaler at firmasystemansvarlige som velger å aktivere DriveLock, også fastsetter en konsernpolitikk for etablering og vedlikehold av master-passord. Dette bør gjøres for å forhindre en situasjon der en ansatt med hensikt eller utilsiktet etablerer begge DriveLock-passordene før han forlater selskapet. Hvis dette skulle skje, ville harddisken bli ubrukbar og trenge utskifting. Ved at de systemansvarlige ikke etablerer et master-passord kan de likeledes risikere å finne seg utestengt fra en harddisk og ute av stand til å utføre rutinekontroll for uautorisert programvare, andre aktivakontrollfunksjoner og støtte.

For brukere med mindre strenge sikkerhetskrav anbefaler ikke HP å aktivere DriveLock. Brukere i denne kategorien omfatter enkeltbrukere eller brukere som ikke oppbevarer sensitive data på harddiskene sine til vanlig. For disse brukerne er det potensielle tapet av en harddisk som resultat av å glemme begge passordene, mye større enn verdien av de data DriveLock er blitt utviklet for å beskytte. Tilgang til Computer Setup og DriveLock kan begrenses gjennom konfigureringspassordet. Ved å fastsette et konfigureringspassord og ikke gi det til sluttbrukerne, kan de systemansvarlige begrense brukernes mulighet til å aktivere DriveLock.

Smart dekselsensor

Smart dekselsensor, som finnes på enkelte modeller, er en kombinasjon av maskinvare- og programvareteknologi som kan varsle når datamaskinens deksel eller sidepanel er blitt fjernet. Det er tre beskyttelsesnivå, som beskrevet i tabellen nedenfor:

Beskyttelsesnivåer for Smart dekselsensor

Nivå	Innstilling	Beskrivelse
Nivå 0	Disabled	Smart dekselsensor er deaktivert (standard).
Nivå 1	Varsle bruker	Når datamaskinen startes på nytt, vises en melding på skjermen som indikerer at datamaskinens deksel eller sidepanel er blitt fjernet.
Nivå 2	Konfigureringspassord	Når datamaskinen startes på nytt, vises en melding på skjermen som indikerer at datamaskinens deksel eller sidepanel er blitt fjernet. Du må oppgi konfigureringspassordet for å fortsette.



Disse innstillingene kan endres med bruk av Computer Setup. Hvis du ønsker mer informasjon om Computer Setup, kan du se i håndboken *Computer Setup (F10) Utility Guide*.

Angi beskyttelsesnivå for Smart dekselsensor

Slik angir du beskyttelsesnivå for Smart dekselsensor:

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Velg **Security** og deretter **Smart Cover** og følg anvisningene på skjermen.
4. Før du avslutter, klikker du på **File > Save Changes** og **Exit**.

Smart deksellås

Smart deksellås er en programvarestyrt deksellås som finnes på enkelte HP-dataskinner. Denne låsen hindrer uautorisert tilgang til de interne komponentene. Dataskinnerne leveres med Smart deksellås i ulåst posisjon.



FORSIKTIG! For å få maksimal sikkerhet for deksellåsen, må du etablere et konfigureringspassord. Konfigureringspassordet hindrer uautorisert tilgang til hjelpeprogrammet Computer Setup.



Smart deksellås er tilgjengelig som et alternativ på enkelte systemer.

Låse Smart-deksellåsen

Gjør følgende når du vil aktivere og låse Smart deksellås:

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på dataskinneren og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Velg **Security** og deretter **Smart Cover** og alternativet **Locked**.
4. Før du avslutter, klikker du på **File > Save Changes** og **Exit**.

Låse opp Smart-deksellåsen

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på dataskinneren og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Velg **Security > Smart Cover > Unlocked**.
4. Før du avslutter, klikker du på **File > Save Changes** og **Exit**.

BrUSE Smart FailSafe dekselnøkkel

Hvis du aktiverer Smart deksellås og du ikke kan angi passordet for å deaktivere låsen, trenger du en Smart FailSafe dekselnøkkel når du skal åpne dekselet på datamaskinen. Denne nøkkelen vil du få bruk for under følgende omstendigheter:

- Strømstans
- Oppstartssvikt
- PC-komponentfeil (som f.eks. prosessor eller strømforsyning)
- Glemt passordet



FORSIKTIG! Smart FailSafe dekselnøkkel er et spesialisert verktøy som leveres av HP. Vær forberedt; bestill denne nøkkelen før du trenger en hos en autorisert forhandler eller tjenesteleverandør.

Du kan skaffe deg FailSafe-nøkkelen på en av følgende måter:

- Kontakt en autorisert HP-forhandler eller serviceleverandør.
- Ring nummeret som gjelder for deg, i garantien.

Hvis du vil ha mer informasjon om bruk av FailSafe-dekselnøkkelen, kan du slå opp i *Hardware Reference Guide*.

Master Boot Record-sikkerhet

Master Boot Record (MBR) inneholder informasjon som trengs for å kunne starte opp fra en disk og få tilgang til dataene som er lagret på harddisken. Master Boot Record Security kan forhindre utilsiktede eller ondsinnede forandringer i MBR, som kan forårsakes av f.eks. datavirus eller av ukorrekt bruk av visse diskverktøy. Den lar deg også gjenopprette den “sist kjente, gode” MBR, hvis det skulle oppdages endringer i MBR når datamaskinen startes på nytt.

Gjør følgende hvis du vil aktivere MBR-sikkerhet:

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Velg **Security > Master Boot Record Security > Enabled**.
4. Velg **Security > Save Master Boot Record**.
5. Før du avslutter, klikker du på **File > Save Changes og Exit**.

Når MBR-sikkerhet er aktivert, forhindrer BIOS at det gjøres forandringer i MBR på gjeldende oppstartbare disk i MS-DOS eller Windows' sikkerhetsmodus.



De fleste operativsystemer kontrollerer tilgangen til MBR på gjeldende oppstartbare disk; BIOS kan ikke forhindre endringer som kan forekomme mens operativsystemet kjører.

Hver gang datamaskinen slås på eller startes på nytt sammenligner BIOS den gjeldende oppstartbare diskens MBR med den tidligere lagrede MBR. Hvis det oppdages endringer, og hvis gjeldende oppstartbare disk er den samme disken som MBR tidligere ble lagret fra, vises følgende melding:

1999 – Master Boot Record has changed.

Trykk på en tast for å starte Setup for å konfigurere MBR-sikkerhet.

I Computer Setup må du

- Lagre den gjeldende oppstartbare diskens MBR;
- Gjenopprette den tidligere lagrede MBR eller
- Deaktivere MBR-sikkerhetsfunksjonen.

Du må kjenne konfigurasjonspassordet, om det finnes.

Hvis det oppdages endringer, og hvis gjeldende oppstartbare disk **ikke** er den samme disken som MBR tidligere ble lagret fra, vises følgende melding:

2000 – Master Boot Record Hard Drive has changed.

Trykk på en tast for å starte Setup for å konfigurere MBR-sikkerhet.

I Computer Setup må du

- Lagre den gjeldende oppstartbare diskens MBR eller
- Deaktivere MBR-sikkerhetsfunksjonen.

Du må kjenne konfigurasjonspassordet, om det finnes.

Hvis den tidligere lagrede MBR mot formodning skulle være ødelagt, vises følgende melding:

1998 – Master Boot Record has been lost.

Trykk på en tast for å starte Setup for å konfigurere MBR-sikkerhet.

I Computer Setup må du

- Lagre den gjeldende oppstartbare diskens MBR eller
- Deaktivere MBR-sikkerhetsfunksjonen.

Du må kjenne konfigurasjonspassordet, om det finnes.

Før du partisjonerer eller formaterer gjeldende oppstartbare disk

Sørg for MBR-sikkerhet er deaktivert før du endrer formatering eller partisjonering av gjeldende oppstartbare disk. Enkelte diskverktøy (som for eksempel FDISK og FORMAT) forsøker å oppdatere MBR. Hvis MBR-sikkerhet er aktivert når du endrer formatering eller partisjonering av disken, vil du kanskje motta feilmeldinger fra diskverktøyet eller en advarsel fra MBR-sikkerhet neste gang datamaskinen slås på eller startes på nytt. Gjør følgende hvis du vil deaktivere MBR-sikkerhet:

1. Slå på maskinen eller start den på nytt. Hvis du er i Windows, klikker du på **Start > Avslutt > Starte maskinen på nytt**.
2. Trykk på **F10**-tasten når lampen på skjermen begynner å lyse grønt. Trykk eventuelt på **Enter** for å omgå tittelskjermbildet.



Hvis du ikke trykker på **F10**-tasten når du skal, må du slå av og på datamaskinen og trykke på **F10**-tasten igjen for å få tilgang til verktøyet.

3. Velg **Security > Master Boot Record Security > Disabled**.
4. Før du avslutter, klikker du på **File > Save Changes** og **Exit**.

Kabellåsutstyr

På bakpanelet på datamaskinen er det plass til en kabellås som gjør at datamaskinen fysisk kan festes til et underlag.

Hvis du vil ha illustrerte instruksjoner, se *Hardware Reference Guide* på *Documentation Library*-CDen.

Teknologi for identifikasjon av fingeravtrykk

Hvis du bruker HPs teknologi for identifikasjon av fingeravtrykk, fjernes behovet for å legge inn brukerpassord. Nettverkssikkerheten skjerpes, påloggingsprosessen forenkles og kostnadene ved å administrere firmanettverk reduseres. Siden den er tilgjengelig til en rimelig pris, er den ikke lenger kun for de ekstremt sikkerhetsbevisste organisasjonene.



Støtte for teknologi for identifikasjon av fingeravtrykk varierer etter modell.

For mer informasjon, besøk

<http://h18000.www1.hp.com/solutions/security>.

Varsling og reparering av feil

Funksjonene for varsling og reparasjon av feil kombinerer ny maskinvare- og programvareteknologi for å hindre tap av kritiske data og redusere uventede driftsavbrudd til et minimum.

Når det oppstår en feil, viser datamaskinen dialogboksen Lokal melding, som beskriver feilen og eventuelle anbefalte løsninger. Du kan vise gjeldende maskinstatus ved å bruke HP Client Manager. Hvis datamaskinen er koblet til et nettverk som styres av HP Insight Manager, HP Client Manager eller andre systemadministrasjonsprogrammer, sender den også varsel om feil til disse programmene.

System for harddiskbeskyttelse

Drive Protection-system (DPS) er et diagnoseverktøy som er innebygd i harddiskene som finnes i enkelte HP-PCer. DPS er utformet for å hjelpe deg å diagnostisere problemer som kan føre til utskifting av harddisken som ikke dekkes av garantien.

Når HPs PC-er bygges, brukes DPS til å teste alle installerte harddisker, og registrert nøkkelinformasjon blir permanent skrevet på disken. Testresultater blir skrevet til harddisken hver gang du kjører DPS. Tjenesteleverandøren kan bruke denne informasjonen til å diagnostisere forholdene som gjorde at du kjørte DPS-programmet. Slå opp i *Feilsøking* hvis du vil ha anvisninger om bruk av DPS.

Overspenningstolerant strømforsyning

En integrert overspenningstolerant strømforsyning gir større driftssikkerhet når datamaskinen rammes av plutselig overspenning. Denne strømforsyningen er beregnet å tåle opp til 2000 volts overspenning uten at det fører til stans i systemet og tap av data.

Varmesensor

Varmesensoren er en maskinvare- og programvarefunksjon som overvåker den indre temperaturen i datamaskinen. Funksjonen viser en advarsel når det normale temperaturområdet overskrides, noe som gir deg tid til å sette i verk nødvendige tiltak før indre komponenter skades eller data går tapt.

Register

A

- ActiveUpdate 6
- advarsler
 - beskytte ROM 7
- aktivasporing 20
- Altiris 4
- Altiris PC Transplant Pro 5
- angi
 - konfigureringspassord 26
 - oppstartspassord 25

B

- beskytte harddisk 46
- beskytte ROM, advarsel 7
- bestille FailSafe-nøkkel 42
- bytte operativsystem, viktig informasjon 19

C

- Computer Setup-verktøy 9

D

- deksellås, smart 41
- deksellåssikkerhet, forsiktig 41
- diagnoseverktøy for harddisker 46
- disk, kloning 2
- DiskOnKey
 - se også* HP Drive Key
 - oppstartbar 13 til 18
- distribusjonsverktøy, programvare 2
- Drivelock 37 til 39

E

- endre passord 26
- endringsmelding 6

F

- FailSafe Boot Block ROM 8
- FailSafe-nøkkel
 - bestille 42
 - forsiktig 42
- feilvarsling 46
- fjerne passord 28
- fjerninstallasjon 3
- Fjern-ROM-Flash 7
- Fjernsysteminstallasjon, tilgang til 3
- forhåndsinstallert programvarebilde 2
- formatere disk, viktig informasjon 45
- forsiktig
 - FailSafe-nøkkel 42
 - sikkerhet for deksellås 41
- første konfigurering 2

G

- gjenopprette krypterte data 33 til 37
- gjenopprette system 8
- gjenoppretting, programvare 2
- gjenoppretting, ProtectTools 33 til 37

H

- harddisker, diagnoseverktøy 46
- HP Client Manager 4
- HP Drive Key
 - se også* DiskOnKey oppstartbar 13 til 18

I

innebygd sikkerhet, ProtectTools 29 til 37
innvendig temperatur i datamaskinen 47
Internett-adresser, Se Nettsteder

K

kabellås-utstyr 45
kloningsverktøy, programvare 2
konfigurere passord
 innstilling 24
konfigurere strømbryter 18
konfigurering
 første 2
konfigureringspassord
 angi 26
 endre 26
 ProtectTools 30
 slette 27
kontrollere tilgang til datamaskinen 20

L

låse opp Smart deksellås 41
låsing av Smart deksellås 41

M

Master Boot Record Security 43 til 44
melding om endringer 6
Multibay-sikkerhet 37 til 39

N

nasjonale tastaturskille tegn 28
Nettsteder
 ActiveUpdate 6
 Altiris 5
 Altiris PC Transplant Pro 5
 Fingerprint Identification Technology 46
 Finterprint Identification Technology 46
 Fjern-ROM-Flash 7
 HPQFlash 8
 kopiere setup 12
 Proactive Change Notification 6

programvarestøtte 19
ROMPaq-bilder 7
System Software Manager (SSM) 6

nettsteder

 PC-distribusjon 2
 ROM-Flash 7

O

operativsystemer, viktig informasjon om 19
oppgradere ROM 7
oppstartbar disk, viktig informasjon 45
oppstartbar enhet
 diskett 12
 DiskOnKey 13 til 18
 HP Drive Key 13 til 18
 opprette 12 til 17
 USB Flash Media-enhet 13 til 18
oppstartspassord
 angi 25
 endre 26
 slette 27
overspenningstolerant strømforsyning 47

P

partisjonere disk, viktig informasjon 45
passord
 endre 26
 fjerne 28
 konfigurering 24, 26
 oppstart 25
 ProtectTools 30 til 33
 sikkerhet 24
 slette 27
PCN (Proactive Change Notification) 6
Preboot Execution Environment (PXE) 3
Proactive Change Notification (PCN) 6
programvare
 aktivasporing 20
 Computer Setup-verktøy 9
 Drive Protection System 46

- FailSafe Boot Block ROM 8
- Fjern-ROM-Flash 7
- Fjernsysteminstallasjon 3
- gjenoppretting 2
- integrasjon 2
- Master Boot Record Security 43 til 44
- oppdatere flere maskiner 6
- System Software Manager 6
- Varsling og reparering av feil 46
- ProtectTools Embedded Security 29 til 37
 - gjenoppretting 33 til 37
 - gjenopprettingsnøkkel 31
 - passord
 - Basic User 32
 - Emergency Recovery Token 31
 - konfigurerings 30
 - Take Ownership 31
- PXE (Preboot Execution Environment) 3

R

ROM

- Fjern-Flash 7
- oppgradere 7
- tastaturlamper, tabell 9
- ugyldig 8

S

setup

- kopiere 9

sikkerhet

- DriveLock 37 til 39
- funksjoner, tabell 21
- innstillinger, stille inn 20
- Master Boot Record 43 til 44
- MultiBay 37 til 39
- passord 24
- ProtectTools 29 til 37
- Smart deksellås 41 til 42

- Smart dekselsensor 40
- skilletegn, tabell 28
- slette passord 27
- Smart deksel FailSafe-nøkkel, bestille 42
- Smart deksellås 41 til 42
 - låse 41
 - låse opp 41
- Smart dekselsensor 40
 - beskyttelsesnivåer 40
 - innstilling 40
- stasjon, beskytte 46
- strømbryter
 - dobbeltfunksjon 18
 - konfigurere 18
- strømbryter med dobbelt funksjon 18
- strømforsyning, overspenningstolerant 47
- System Software Manager (SSM) 6
- systemgjenoppretting 8

T

- tastaturlamper, ROM, tabell 9
- tastaturskilletegn, nasjonale 28
- teknologi for identifikasjon av fingeravtrykk 46
- temperatur, innvendig i datamaskinen 47
- tilgang til datamaskinen, kontrollere 20
- tilpasse programvare 2

U

- ugyldig system-ROM 8
- URLer (nettsteder). Se nettsteder
- USB Flash Media-enhet, oppstartbar 13 til 18

V

- varmesensor 47

W

Web-områder

- HP Client Manager 4